(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 898 595 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
12.03.2008 Bulletin 2008/11

(51) Int Cl.:
H04L 29/06 *(2006.01)* ***H04L 12/58*** *(2006.01)*

(21) Application number: **07253525.5**

(22) Date of filing: **06.09.2007**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(30) Priority: **08.09.2006 US 518071**

(71) Applicant: **Iconix, Inc.**
Santa Clara, CA 95054 (US)

(72) Inventors:
- **Zager, Robert Philip**
  Saratoga,
  California 95070 (US)
- **Picazo, Jose Jesus**
  Livermore,
  California 94550 (US)
- **Vempaty, Nageshwara Rao**
  Palo Alto,
  California 94306 (US)
- **Ames, William**
  San Jose,
  California 95135 (US)
- **Duvvoori, Vikram**
  Salinas,
  California 93907 (US)

(74) Representative: **Maury, Richard Philip**
Marks & Clerk
90 Long Acre
London WC2E 9RA (GB)

(54) Rapid identification of message authentication

(57) Techniques are presented for uniquely identifying authentication associated with messages. A message is inspected for sender or domain identifying information associated with a sender of the message or a sender's domain. The identifying information is authenticated, and if authentication, then distinctive metadata is associated with the message. The distinctive metadata is presented or played in connection with the message for purposes of readily identifying the authentication.

EP 1 898 595 A1

Description

Field

[0001] The invention relates generally to network security and more particularly to message authentication mechanisms.

Background

[0002] Electronic mail (email) communication is becoming increasingly pervasive throughout the world. Enterprises rely on email to conduct business, governments rely on email to communicate, and individuals rely on email to conduct their affairs.

[0003] In recent years, email communication has expanded to include Instant Messaging (IM) and Text Messaging. Communications now use any computer (processing device) or combination of portable devices that may interact wirelessly or interact over a combination of wired and wireless networks. Some techniques also use groupware where more than two or more people interact with one another via direct communications. These techniques present real-time or near real-time communication with individuals via their portable devices, such as Personal Digital Assistants (PDA's), phones, *etc.* IM has also become popular in virtual communities, where members interact with one another electronically in user-formed communities, associations, or groups.

[0004] Unfortunately, mass marketers and nefarious individuals have watered down the usefulness of email communication. That is, spam, Phishing techniques, and even computer viruses are now regularly proliferated via email. As a result, many individuals and entities have invested in expensive filtering mechanisms and/or have limited the extent to which they may view their messages. In some cases, individuals may even carry multiple email accounts and may only view some of their email accounts on a very infrequent basis. These situations make it difficult for legitimate enterprises to reach their customers/clients.

[0005] In effect, individuals have become desensitized to their email because their inboxes are bursting with far too many junk emails of no value to them or even worse potentially harmful to them. Harmful emails can include such things as viruses that damage a users' device or files or Phishing emails that link a user to a bogus World-Wide Web (WWW) site for purposes of obtaining confidential information about the user. The latter technique is often used to illegally access financial accounts and/or to assume an online identity of a user.

Summary

[0006] In various embodiments, techniques are presented for rapid identification of message authentication. In one embodiment a method is provided that identifies a message directed to a recipient and determines when the message includes identifying information associated with a sender of that message. When the identifying information is present, an external service is requested to authenticate an identity of the sender and to provide distinctive metadata with the message for purposes of uniquely identifying the sender to the recipient.

Brief Description of the Drawings

[0007] FIG. 1 is a diagram of method for rapidly identifying message authentication, according to an example embodiment.

[0008] FIG. 2 is a diagram of another method for rapidly identifying message authentication, according to an example embodiment.

[0009] FIG. 3 is a diagram of a message authentication system, according to an example embodiment.

Detailed Description

[0010] FIG. 1 is a diagram of method 100 for rapidly identifying message authentication, according to an example embodiment. The method 100 (hereinafter "message authentication service") is implemented as instructions in a machine-accessible and readable medium. The instructions when accessed by a machine perform the processing depicted in FIG. 1. The message authentication service is also operable over a network, and the network may be wired, wireless, or a combination of wired and wireless.

[0011] Initially, a message, such as an electronic mail (email), message is constructed by a sender using a sender's message client or messaging service and is sent over a network, such as the Internet, to a recipient. The header information associated with the message can include a variety of information that the message authentication service may subsequently detect and use for purposes of ensuring that the message is authenticated.

[0012] For example, the message may include a signature, a key, such as a public key of a domain or of a specific sender. Alternatively, the message may include a serial number. In some cases, the message may just include the domain path from an originating sender's messaging server that the message originated from. In still other situations, the header may include a variety or multiple types of information that may be relevant to authentication of either the sender or the domain of the sender.

[0013] The message client of the sender may or may not be modified to include the additional information (herein referred to as "identifying information") included in the header of a message. That is, the message client may be designed to cooperate and supply information expected by the message authentication service or the message client may be completely unaware of the message authentication service and may construct and send messages in a normal fashion having normal header information assembled by the sender's messaging client.

[0014] When the message is received on or within the environment of the recipient of the message, the message authentication service intercepts and initially inspects the message. This may be achieved via a prior configuration with the messaging client of the recipient or may be achieved via a reverse or transparent proxy arrangement, where the message authentication service operates unbeknownst to the recipient's messaging client and intercepts and inspects headers of received messages, which are directed to a recipient.

[0015] The processing of the message authentication service is designed to rapidly authenticate a received message's sender and/or a sender's domain. It is noted that only identified domains or senders may be authenticated and inspected by the message authentication service. That is, some messages may process normally in the recipient's messaging client without authentication techniques (described more completely below) being performed by the message authentication service. The specific senders or domains that are authenticated may be identified according to custom rules or policies. This permits some messages to process normally whereas others are selectively processed in the manners described more completely below.

[0016] With this initial context, the processing of the message authentication service will now be discussed with reference to FIG. 1. At 110, the message authentication service identifies a message that is being directed to a recipient. This identification process may occur in a variety of manners. For example, the message authentication service may intercept the message before it is received by a messaging client of the recipient. Alternatively, the message authentication service may cooperate and integrate with at least some processing of the recipient's messaging client to detect and identify the received message.

[0017] At 120, the message authentication service determines when a message includes identifying information that the message authentication service is interested in knowing about. The identifying information may, at 121, be located, detected, or discovered according to rules or policies, and these rules or policies may be associated with a specific sender, a specific domain, and/or a specific recipient. In some cases, at 122, the identifying information is detected by inspecting the header of a message for a key, a signature, serial number, or various combinations of these things representing the identifying information. It is also noted that the identifying information may be a path for a domain or may be a custom hash or encryption key as well. The identifying information was previously inserted by the messaging client of the sender either in normal manners or in a custom manner designed to interact and cooperate with the processing of the message authentication service.

[0018] At 130, the message authentication service makes a request to an external service to authenticate an identity of the sender or an identity of the domain associated with the sender by supplying the identifying information parsed from the message or header of the message. Again, policies or rules may drive the specific identity of the external authentication service and the technique that is to be performed to authenticate the sender or the domain of the sender.

[0019] For example, suppose that the identifying information is a signature associated with America Online, such that America Online or Verisign® can be consulted to acquire a key, which was previously used to generate a signature value that is included in the message header. The independently acquired key is then used to generate an independent signature value from the message text and/or header, which can then be compared to a signature value supplied as the identifying information with the message or message header. If a match occurs than this type of authentication technique may be viewed as successful.

[0020] It is noted that the type of authentication and the level of confidence associated with the authentication are customizable and may be altered according to rules or policies. So, multiple levels of authentication, strong authentication, or weak authentication may be used according to subscription services and rules or policies for any given recipient, sender, and/or domain.

[0021] As another example, consider a message that is encrypted with public and private key encryption. The public key of the recipient may be used in combination with a private key of the sender or domain and used to encrypt the entire message text. The type of authentication may be listed as the identifying information in the header of the message and the message authentication service may consult an external service to decrypt the message using a server-administered private key for the sender or domain. If decryption occurs, then authentication was successful. This type of authentication may be viewed as stronger since dual key encryption is used and since the server administers and maintains the private keys without distributing them and supplies a decryption service that decrypts the encrypted message text on behalf of the recipient. Alternatively, a service may provide the public key and decryption can be done independently by an administrator. For example, decryption could be done locally by a user's or recipient's machine, device, or locally accessible devices.

[0022] In fact, a variety of identifiers and authentication may be used. The degree of complexity and level of security are customizable and can be integrated with the teachings presented herein.

[0023] At 140, the message authentication service provides distinctive metadata that is to be associated with the received message when the identity or domain of the sender is properly authenticated. The distinctive metadata permits a recipient to rapidly discern that the message has been authenticated with respect to either the sender or the domain or both the sender and the domain. Moreover, the distinctive metadata can change over time. For instance, an enterprise may change its logo. So, the distinctive metadata does not have to be viewed as being

static, in some cases policies may permit it to be dynamically updated or altered as needed or desired. It is also noted that the distinctive metadata is displayed within the inbox of the messaging client for the recipient and does not have to be displayed within the message itself.

[0024] For example, at 141, a portion of the distinctive metadata may be a graphic trademark icon or image associated with a domain of the sender. So, if the domain is America Online®, a portion of the distinctive metadata may be a trademark logo image associated with American Online®. It is noted, that the graphical image or icon does not have to be associated with an enterprise, it may just as easily be associated with a specific individual. In some cases, the image or icon may be associated with a specific email address and multiple individuals may share the same email address. So, the degree of specificity may be customized. Graphic image or icon customization may occur at the email level, at email aggregation levels for groups, at the domain level, at sub domain levels, *etc.* Moreover, the specific graphical image or icon may be customized and assigned by either the recipient or the sender according to their own desired profiles. Moreover, multiple domains that are identified with a specific enterprise may be mapped to a single graphical icon or image for that enterprise.

[0025] According to an embodiment, at 142, a variety of more detailed information may also be associated with various other portions of the distinctive metadata. For instance, a specific authentication type, an identity for the sender, an identity for the sender's domain, and/or a date and time that authentication was performed. In fact, the detailed information may also include other related information such as hypertext links to other information or to recipient-defined custom information. The detailed information may be presented when the recipient brings the graphical image or icon into focus within the recipient's messaging client. For example, a mouse may be situated over an icon and when this occurs focus is directed to the distinctive metadata and the additional information is depicted for the recipient to view. In other cases, the graphical icon is selectable such that when it is double-clicked on the detailed information pops up in another window for the recipient to view.

[0026] In fact, the distinctive metadata does not have to exclusively be limited to graphical images. At 150, the metadata may be represented as an audible sound or jingle, a unique vibration, or even a distinct odor. So, the distinctive metadata may be used to drive aspects of devices that may cause the devices to perform some other operation, such as vibrate, play a tune, or emit an odor.

[0027] The point is that the identifying information included and detected with the message is validated or authenticated according to policy or rule and then other policies or rules permit distinctive metadata to be associated with successful validation or authentication. The distinctive metadata is then integrated into features of the recipient's messaging client to rapidly communicate to the recipient that the message is authentic. The degree of information presented and the manner in which the presentation is made is also configurable according to one or more rules or policies.

[0028] In an embodiment, at 160, the recipient's messaging client may also be configured to include distinctive metadata for each message received in spite of the fact that some messages may not actually participate in the authentication process described above. In such scenarios, the message authentication service may produce a generic graphical icon and add it to a non participating message's metadata. This generic graphical icon may be used to rapidly alert the recipient to the fact that a particular message did not undergo the normal authentication process. The recipient may then decide to route such messages to predefined folders for further processing, such as virus scans, spam filters, *etc.,* or may elect to discard or view the messages at the recipient's own peril.

[0029] In this manner, a recipient may be capable of readily discerning from a listing of messages which messages are authenticated and which are not; and, in the case of processing at 150, graphical information that is highly likely to identify the sender (e.g., a bofa logo, etc.) Custom filters or routing algorithms may also be applied in response to the metadata added by the message authentication service, if desired by the recipient. Moreover, each message may be associated with different degrees of authentication and may include custom levels of information in their metadata.

[0030] As an example application, consider a web-based email client that presents a listing of emails along with some message-client supplied metadata, such as sender identification, subject header, date and time received, etc. The processing of the message authentication service may be integrated to sit on top of such a client to alter the presentation of the listing to include customized graphical images and customized metadata for messages that have been authenticated, or in some cases for all messages including those not participating. Each image may rapidly identify for the recipient the identity of the sender and/or the identity of the domain used by the sender. The authentication may include sender and domain, just the domain, or just the sender. A recipient may also mouse over or select any given image and receive other custom information from the custom metadata supplied by the message authentication service. The recipient may also set up filters or routing algorithms to automatically process messages in response to information included in the custom metadata. Such processing permits rapid identification of message authentication from the perspective of the recipient.

[0031] It is also noted, that the message authentication service may actually be a remote service that is not directly installed within the environment of the recipient's message client. In such cases, a proxy may be used to detect messages and forward them to the remote message authentication service for generation of the custom and distinct metadata. Another application may superim-

pose the custom and distinct metadata in views presented by the recipient's message client. So, the message authentication service does not have to be integrated and coupled with the recipient's messaging client; although it can be.

[0032] It is also worth noting that techniques of the message authentication service are not specifically limited to email-based messaging. That is, any type of messaging such as IM and TM may be used and may benefit from the techniques presented herein. For example, a phone's TM or IM capabilities may be augmented to process the message authentication service, such that authentication is rapidly identified via custom vibrations and/or custom sounds and images.

[0033] FIG. 2 is a diagram of another method 200 for rapidly identifying message authentication, according to an example embodiment. The method (hereinafter referred to a "message authentication identifying service") is implemented as instructions in a machine-accessible and readable medium and is accessible over a network. The network may be wired, wireless, or a combination of wired and wireless. The instructions when accessed by a machine perform the processing depicted in FIG. 2. The message authentication identifying service presents an alternative processing perspective to what was presented above with respect to the method 100 of the FIG. 1.

[0034] At 210, the message authentication identifying service receives an email message from a sender. Again, receipt of this email may occur in a variety of manners, such as direct forwarding from a recipient's email client, interception of the message before being received by the recipient's email client, and the like.

[0035] At 220, the message authentication identifying service externally authenticates the sender and/or domain of the sender. That is, the message authentication identifying service enlists the services of an external system or application to provide an indication that the email received is in fact from a sender that it purports to be sent from and/or is in fact coming from a domain that is trusted or known to be associated with the sender or from an entity that the message authentication identifying service trusts.

[0036] According to an embodiment, at 221, the particular authentication service that the message authentication identifying service enlists help from may be selected in response to a dynamically evaluated rule or policy. So, the message authentication identifying service may dynamically and in real time determine the identity of the authentication service to request authentication from. Determination for the rule or policy may be based on a variety of factors, such as the perceived identity of the sender, the perceived identity of the domain, a license agreement between the recipient and the message authentication identifying service, and the like.

[0037] At 230, the message authentication identifying service associates distinctive metadata for any authenticated sender and/or domain. Custom and distinctive metadata is generated, acquired, or assigned to the email in response to successful authentication. According to an embodiment, at 231, this may entail acquiring the metadata according to rules associated with the sender, the recipient, and/or the domain of the sender.

[0038] In an embodiment, at 232, the metadata may be represented in a variety of different manners or in a combination of manners. So, the metadata may be represented as a graphical icon image, an audible sound, a vibration, an odor, or various combinations of these things.

[0039] At 233, the metadata may also be represented as a composite data structure so as to include a variety of additional beneficial information. For example, the composite data structure may include custom information types that identify various types of information included within the metadata (e.g., hypertext links, images, sounds, *etc.*). In some cases, the schema associated with the metadata may be represented in as a Extensible Markup Language (XML) Schema Definition (XSD). This permits subsequent applications to automatically parse, recognize, integrate, and utilize the composite data structure in an automatic, dynamic and real-time fashion.

[0040] In still more embodiments, at 234, the message authentication identifying service may represent different portions of the metadata to identify the sender, the external authenticator (external authentication service used), and/or the domain of the sender. So, the metadata may include a variety of useful information that the recipient may view or acquire in a variety of custom manners.

[0041] At 240, the message authentication identifying service presents the distinctive metadata, or at least a portion of the distinctive metadata, in connection with one or more views of the email message that is provided to the recipient. For example, at 250, a portion of the custom metadata may be a graphical icon associated with the identity of either the sender or the domain of the sender or both. The graphical icon is presented for viewing by the recipient within a summary or listing view of the recipient's email inbox.

[0042] FIG. 3 is a diagram of a message authentication system 300, according to an example embodiment. The message authentication system 300 is implemented in a machine-accessible and readable medium and is accessible over a wired, wireless, or a combination of wired and wireless networks. The message authentication system 300 implements, among other things, the methods 100 and 200 presented above with reference to the FIGS. 1 and 2.

[0043] The message authentication system 300 includes a message authentication service 301 and a distinctive metadata service 302. Each of these will now be discussed in turn.

[0044] The message authentication service 301 operates on top of or within an environment of a recipient's message client. As messages are received within the environment of the recipient, the message authentication service 301 is activated either directly or indirectly, such

as via calls from a proxy (reverse or transparent proxy). The message authentication service 301 interacts with one or more external authentication services for purposes of authenticating messages received with respect to the identity of the sender, contents of the message itself, and/or the identity of the sender's domain. Example processing for parsing identifying information from messages and enlisting such services were discussed above in detail with respect to the methods 100 and 200 of the FIGS. 1 and 2, respectively.

[0045] The contents of the messages may be authenticated by validating signatures supplied as identifying information with the messages. Another example of this would be to decrypt encrypted messages, validate keys, validate serial numbers, etc. So, authentication may occur with respect to the sender, the domain, or the contents (with successful third party decryption of the contents), or combinations of all three of these items.

[0046] In some cases, the message authentication service 301 intercepts or acquires messages and enlists the services of one or more external authentication services to authenticate messages before these messages are presented to a recipient within a recipient's email or message client. It is noted that only selective messages have to be processed by the message authentication service 301; that is, some messages may not be processed or may be ignored or generically processed by the message authentication service 301. Such scenarios were described above with respect to the method 100 and the FIG. 1. This may occur when a recipient desires that only certain domains or senders are to be processed or when a recipient desires to have all non participating senders or domains to be processed in a uniform manner so as to be readily identified by the recipient.

[0047] In other cases, the message authentication service 301 may be configured to request the external authentication or the messages when specifically requested to do so by a recipient and/or after the messages are viewed or accessible to the recipient. So, authentication does not have to occur before the messages are processed; although this can occur in some embodiments.

[0048] The message authentication service 301 interacts with the distinctive metadata service 302 for purposes of communicating authenticated senders, domains, or message contents. The distinctive metadata service 302 may use one or more custom-defined rules or policies to generate or acquire distinctive metadata to associate with authenticated messages.

[0049] According to an embodiment, the distinctive metadata service 302 is external to the message authentication service 301. So, the distinctive metadata service 302 may be its own distinct and generic server-based service that can be dynamically consulted and interacted with.

[0050] The distinctive metadata service 302 generates custom information for an authenticated message that is associated with metadata for that message. The information may be a graphic icon or it may be a combination of information. Additionally, the information may be a sound, a vibration, an odor, and the like. At least a portion of the information is presented with the message and summary listings of the message within the recipient's message client for purposes of permitting the recipient to rapidly identify the message's authentication. Other portions of the information may be acquired and brought into focus by the recipient or when specifically requested by the recipient.

[0051] In some cases, the distinctive metadata service 302 may provide generic metadata for messages not associated with the authentication of the message authentication service 301. So, each message not processed by the message authentication service 301 may receive its own generic identifying information.

[0052] Example processing associated with the distinctive metadata service 302 and the message authentication service 301 were presented above with respect to the methods 100 and 200 of the FIGS. 1 and 2.

[0053] It is also noted that the metadata may be include a variety of information that may be used to automatically filter or process the messages. Additionally, the messaging clients may include email, IM, and/or TM. The degree or authentication and level of metadata information and the manner in which it is presented with a message are all customizable and may be dynamically resolved according to rule or policy.

[0054] The above description is illustrative, and not restrictive. Many other embodiments will be apparent to those of skill in the art upon reviewing the above description. The scope of embodiments should therefore be determined with reference to the appended claims, along with the full scope of equivalents to which such claims are entitled.

[0055] The Abstract is provided to comply with 37 C.F.R. §1.72(b) and will allow the reader to quickly ascertain the nature and gist of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims.

[0056] In the foregoing description of the embodiments, various features are grouped together in a single embodiment for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting that the claimed embodiments have more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus the following claims are hereby incorporated into the Description of the Embodiments, with each claim standing on its own as a separate exemplary embodiment.

Claims

1. A method, comprising:

identifying a message directed to a recipient;
determining when the message includes identifying information associated with a sender of the message;
requesting an external service to authenticate an identity of the sender when the identifying information is present; and
providing, when the identity is authenticated by the external service, distinctive metadata with the message to uniquely identify the sender to the recipient before the recipient opens the message.

2. The method of claim 1 further comprising at least one of:

presenting the distinctive metadata as a unique graphical icon in a summary listing for the message;
playing the distinctive metadata as an audible jingle when the message is inserted into a message queue of the recipient;
activating a device to emit a unique vibration associated with the distinctive metadata when the message is inserted into the message queue of the recipient; and
causing a distinctive odor to be emitted in response to the distinctive metadata when the message is inserted into the message queue of the recipient.

3. The method of claim 1, wherein determining further includes locating the identifying information according to rules associated with at least one of the sender, the recipient, and a domain associated with the message.

4. The method of claim 3, wherein providing further includes representing at least a portion the distinctive metadata as a graphic trademark associated with the sender or the domain of the sender.

5. The method of claim 4 further comprising, presenting more detailed information associated with the metadata when the graphic trademark is brought into focus by the recipient, and wherein the more detailed information includes at least one of a type of authentication used by the external service, an external service identity, a date and a time when authentication was performed by the external service, a hypertext link to additional information, and custom information defined according to one or more rules.

6. The method of claim 1, wherein determining further includes inspecting a header of the message for at least one of a signature, a key and a serial number, which represents the identifying information.

7. The method of claim 1 further comprising, adding a generic graphical icon to the distinctive metadata when the message does not include the identifying information, and wherein the generic graphical icon is presented with the message to the recipient to permit the recipient to determine that no authentication took place with the message.

8. A method, comprising:

receiving an electronic mail (email) message from a sender;
externally authenticating the sender;
associating distinctive metadata for the authenticated sender; and
presenting the distinctive metadata in connection with one or more views of the email message provided to a recipient of the email message.

9. The method of claim 8, wherein associating further includes acquiring the distinctive metadata according to one or more rules associated with at least one of the sender, the recipient, and a domain of the sender.

10. The method of claim 8, wherein associating further includes representing the distinctive metadata as at least one of a unique graphical icon, a unique audible sound, a unique vibration, and a unique odor.

11. The method of claim 8, wherein associating further includes representing the distinctive metadata as composite data structure including custom types of information, wherein each different custom type of information is presented to the recipient according to a state associated with the distinctive metadata.

12. The method of claim 8, wherein externally authenticating further includes selecting an authentication service to perform authentication in response to a rule or policy.

13. The method of claim 8, wherein associating further includes representing different portions of the distinctive metadata to identify at least one of an identity of the sender, an identity of an external authenticator, and an identity of a domain of the sender.

14. The method of claim 8, wherein presenting further includes presenting the distinctive metadata as a custom graphical icon associated with a domain of the sender within a summary view of the recipient's email inbox.

15. A system, comprising:

a message authentication service; and
a distinctive metadata service, wherein the mes-

sage authentication service is to identify emails having identifying information and to request authentication for senders of the emails, and wherein the message authentication service is to interact with the distinctive metadata service for authenticated senders to acquire and present custom and distinctive metadata for each authenticated sender in a message client associated with a recipient.

16. The system of claim 15, wherein the distinctive metadata service is external to the message authentication service.

17. The system of claim 15, wherein the message authentication service interacts with one or more external authentication services to perform authentication on the emails.

18. The system of claim 15, wherein the message authentication service is to intercept emails sent to the message client and request the authentication of the senders before the emails are processed by the message client and before the emails are viewable by the recipient within the message client.

19. The system of claim 15, wherein the distinctive metadata service is to provide generic metadata for any senders not authenticated, and wherein the message client is adapted to present the generic metadata with the appropriate emails associated with non authenticated senders.

20. The system of claim 15, wherein the custom and distinct metadata includes at least one of a custom graphical icon, a unique vibration, a unique sound, and a unique odor.

21. The system of claim 15, wherein the message authentication service is to request the authentication of the senders after the emails are presented and accessible to the recipient.

22. A method, comprising:

receiving an electronic mail (email) message from a sender;
externally authenticating the sender;
associating distinctive metadata for the authenticated sender; and
using the distinctive metadata to separate or filter other email messages and the email message provided to a recipient into categories, folders, or buckets of information.

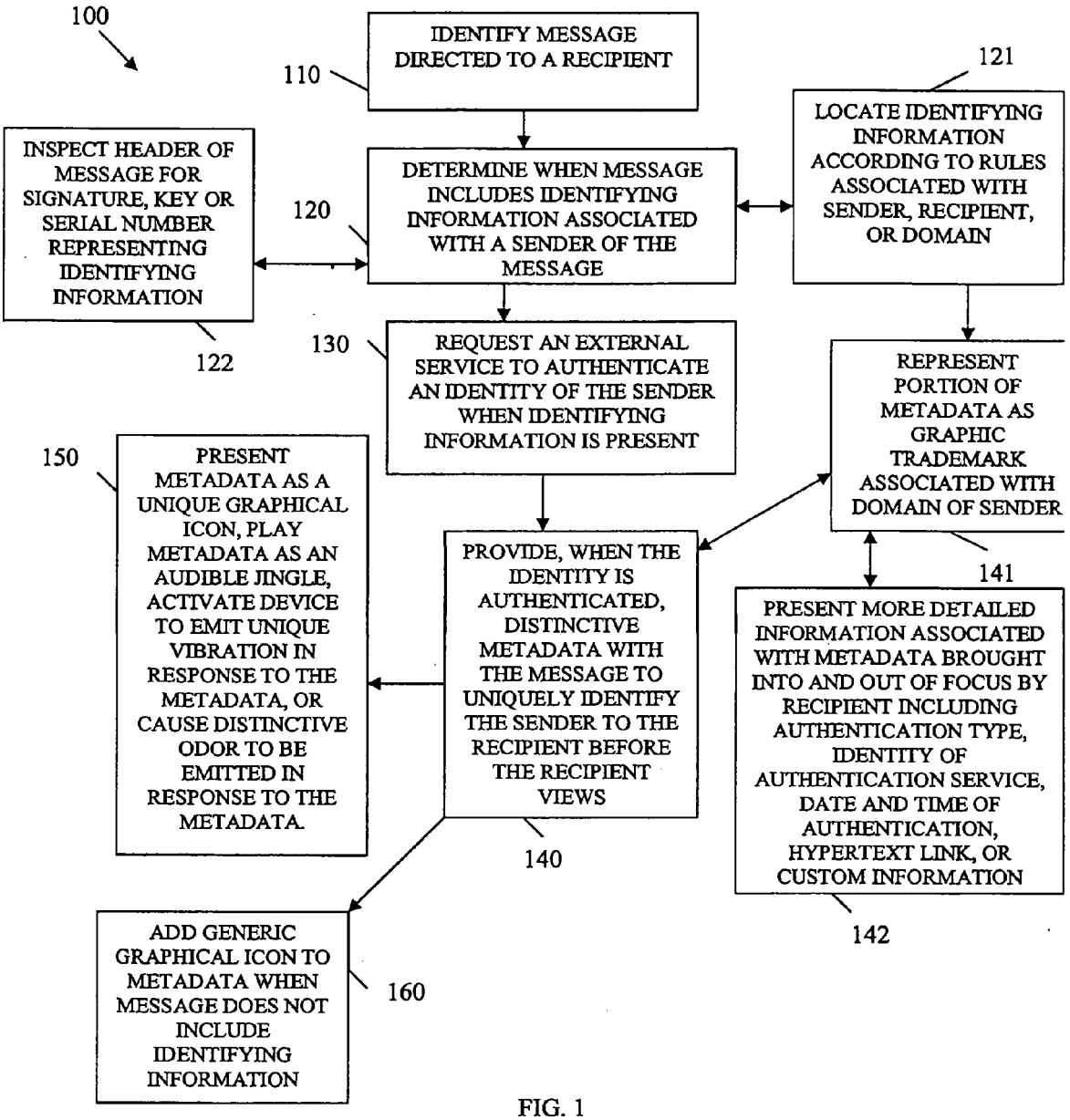
100
IDENTIFY MESSAGE DIRECTED TO A RECIPIENT
110
INSPECT HEADER OF MESSAGE FOR SIGNATURE, KEY OR SERIAL NUMBER REPRESENTING IDENTIFYING INFORMATION
122
DETERMINE WHEN MESSAGE INCLUDES IDENTIFYING INFORMATION ASSOCIATED WITH A SENDER OF THE MESSAGE
120
LOCATE IDENTIFYING INFORMATION ACCORDING TO RULES ASSOCIATED WITH SENDER, RECIPIENT, OR DOMAIN
121
REQUEST AN EXTERNAL SERVICE TO AUTHENTICATE AN IDENTITY OF THE SENDER WHEN IDENTIFYING INFORMATION IS PRESENT
130
REPRESENT PORTION OF METADATA AS GRAPHIC TRADEMARK ASSOCIATED WITH DOMAIN OF SENDER
141
150
PRESENT METADATA AS A UNIQUE GRAPHICAL ICON, PLAY METADATA AS AN AUDIBLE JINGLE, ACTIVATE DEVICE TO EMIT UNIQUE VIBRATION IN RESPONSE TO THE METADATA, OR CAUSE DISTINCTIVE ODOR TO BE EMITTED IN RESPONSE TO THE METADATA.
PROVIDE, WHEN THE IDENTITY IS AUTHENTICATED, DISTINCTIVE METADATA WITH THE MESSAGE TO UNIQUELY IDENTIFY THE SENDER TO THE RECIPIENT BEFORE THE RECIPIENT VIEWS
140
PRESENT MORE DETAILED INFORMATION ASSOCIATED WITH METADATA BROUGHT INTO AND OUT OF FOCUS BY RECIPIENT INCLUDING AUTHENTICATION TYPE, IDENTITY OF AUTHENTICATION SERVICE, DATE AND TIME OF AUTHENTICATION, HYPERTEXT LINK, OR CUSTOM INFORMATION
142
ADD GENERIC GRAPHICAL ICON TO METADATA WHEN MESSAGE DOES NOT INCLUDE IDENTIFYING INFORMATION
160

FIG. 1

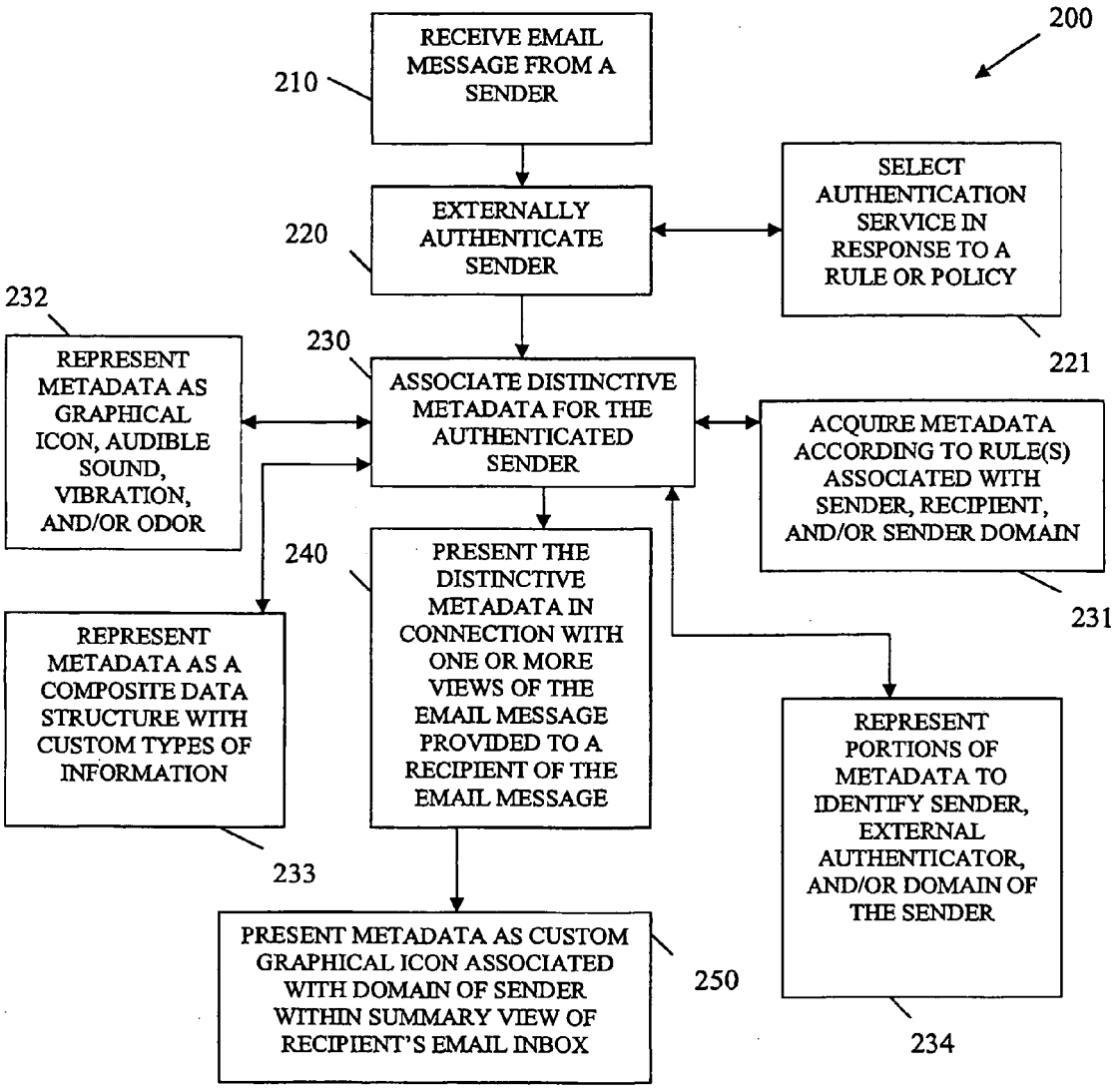
200
RECEIVE EMAIL MESSAGE FROM A SENDER
210
EXTERNALLY AUTHENTICATE SENDER
220
SELECT AUTHENTICATION SERVICE IN RESPONSE TO A RULE OR POLICY
221
232
REPRESENT METADATA AS GRAPHICAL ICON, AUDIBLE SOUND, VIBRATION, AND/OR ODOR
230
ASSOCIATE DISTINCTIVE METADATA FOR THE AUTHENTICATED SENDER
ACQUIRE METADATA ACCORDING TO RULE(S) ASSOCIATED WITH SENDER, RECIPIENT, AND/OR SENDER DOMAIN
231
240
PRESENT THE DISTINCTIVE METADATA IN CONNECTION WITH ONE OR MORE VIEWS OF THE EMAIL MESSAGE PROVIDED TO A RECIPIENT OF THE EMAIL MESSAGE
REPRESENT METADATA AS A COMPOSITE DATA STRUCTURE WITH CUSTOM TYPES OF INFORMATION
233
REPRESENT PORTIONS OF METADATA TO IDENTIFY SENDER, EXTERNAL AUTHENTICATOR, AND/OR DOMAIN OF THE SENDER
234
PRESENT METADATA AS CUSTOM GRAPHICAL ICON ASSOCIATED WITH DOMAIN OF SENDER WITHIN SUMMARY VIEW OF RECIPIENT'S EMAIL INBOX
250

FIG. 2

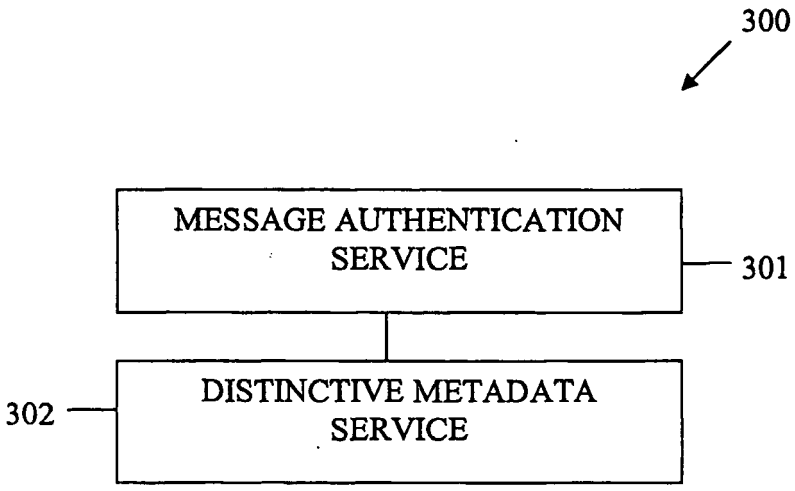
300
MESSAGE AUTHENTICATION SERVICE
301
DISTINCTIVE METADATA SERVICE
302

FIG. 3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 07 25 3525

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
Y	US 2005/182938 A1 (SESHADRI HARISH [US] ET AL) 18 August 2005 (2005-08-18) * paragraphs [0006], [0007] * * paragraphs [0022] - [0037] * * paragraphs [0040] - [0073] * * figure 4 * * claims 12-17 *	1-22	INV. H04L29/06 H04L12/58
Y	WO 03/001326 A (TUMBLEWEED COMM CORP [US]) 3 January 2003 (2003-01-03) * page 9, line 9 - page 13, line 4 * * page 16, line 8 - page 17, line 2 * * page 18, line 7 - page 22, line 19 *	1-22	
Y	WO 01/95588 A (AMERICA ONLINE INC [US]; YOUSTRA WILLIAM N [US]) 13 December 2001 (2001-12-13) * page 1, line 16 - page 2, line 26 * * page 18, line 6 - page 21, line 20 * * figure 8 *	7	
A	US 2002/116508 A1 (KHAN SAL [CA] ET AL) 22 August 2002 (2002-08-22) * paragraphs [0051] - [0080] *	1-22	TECHNICAL FIELDS SEARCHED (IPC) H04L G06Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	19 November 2007	Olaechea, Javier

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 07 25 3525

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

19-11-2007

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005182938 A1	18-08-2005	AU 2005206907 A1	04-08-2005
		BR PI0506876 A	12-06-2007
		CA 2553483 A1	04-08-2005
		EP 1712031 A2	18-10-2006
		WO 2005069867 A2	04-08-2005
WO 03001326 A	03-01-2003	AU 2002345739 A1	08-01-2003
WO 0195588 A	13-12-2001	AU 6678401 A	17-12-2001
		US 2002013902 A1	31-01-2002
US 2002116508 A1	22-08-2002	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82